Conference of State Bank Supervisors™
"Champions of the State Banking System Since 1902"
www.csbs.org

HOW TO COMPLY WITH THE NEW INFORMATION SECURITY STANDARDS:

A "DO IT YOURSELF" MANUAL FOR COMMUNITY BANKS AND THRIFTS

PREPARED FOR THE

CONFERENCE OF STATE BANK EXAMINERS

By

THE CODA GROUP, INC.

BARNETT SIVON & NATTER, P.C. & THOMAS O'DEA

1155 15TH Street N.W.

Suite 1101

Washington DC 20005

(202) 463-6040

HOW TO COMPLY WITH THE NEW INFORMATION SECURITY STANDARDS: A "DO IT YOURSELF" MANUAL FOR COMMUNITY BANKS AND THRIFTS

HOW TO COMPLY WITH THE NEW INFORMATION SECURITY STANDARDS:

A "DO IT YOURSELF" MANUAL FOR COMMUNITY BANKS AND THRIFTS

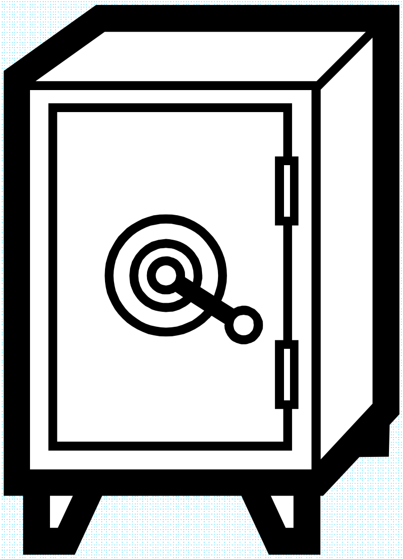
This is a "how to" manual for community banks and thrift institutions struggling with the new guidelines on information security issued by the Federal banking agencies. Rather than providing general guidance, this manual will give you detailed and practical advice on how to comply with these new mandates, and will contain information on what bank examiners will actually look for and care about. However, before we get into the details of how to comply, we will start with some general background information.

BASIC BACKGROUND

The genesis for the current regulatory emphasis on information security can be traced to the Gramm-Leach-Bliley Act of 1999 ("GLBA"). GLBA included the first statutory requirement for the banking agencies to issue information security standards. In addition, section 216 of the Fair and Accurate Credit Transactions Act requires the Federal banking agencies to adopt a regulation to ensure that information derived from consumer reports is disposed of properly. The Federal agencies implemented these statutory requirements by issuing interagency guidelines establishing information security standards in 2001, with revisions in 2004, 2005 and 2006 ("Guidelines"). Customer information security differs from financial privacy in that security measures are designed to safeguard against unauthorized access or use of customer information, while financial privacy rules address a financial institution's ability to disclose data. The topics are related, but not identical.

The Guidelines require financial institutions to develop and maintain a customer information security program. The security program must be a written plan that identifies risks and controls. Financial institutions using outside service providers must have written contractual assurances regarding information handling and security. Essentially, the service providers have to promise to follow supervisory guidelines in this area. This is especially important with respect to community financial organizations that often outsource their data processing needs.

In general, the security guidelines apply to all nonpublic personal ***customer*** information that a financial institution possesses.[1] For example, the guidelines apply to information included in a loan application, deposit information, credit card account, or even the mere fact that the person is a customer of the bank. However, aggregated data and other information that cannot, in any way, be linked to a customer or to an account number are not covered. Also, publicly available information, such as that found in county property records, is exempt. So, for example, a financial institution must safeguard loan data of its customers, but would not have to protect a list of delinquent taxpayers that is available from the county clerk's office. As will be explained below, different rules apply to information disposal safeguards.



[1] A "customer" is defined as a consumer who has a *continuing relationship* with the bank for the provision of financial services.

ESTABLISHING YOUR CUSTOMER INFORMATION SECURITY PROGRAM

A. OBJECTIVE OF PROGRAM

The Guidelines require all banking institutions to have a written information security program that is designed to meet four objectives:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats or hazards to the security or integrity of customer information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
- Ensure the proper disposal of information.

B. BOARD INVOLVEMENT REQUIRED

The institution's board of directors or a committee of the board must approve the program and the security policies. Additionally, the board or committee must also be involved in overseeing and re-evaluating the implementation and ongoing functioning of the plan, including assigning specific responsibility for implementation and management of the program.

C. SCOPE OF PROGRAM

The program must deal with the following issues: assessing risk, managing and controlling risk, overseeing service providers, adjustments, reporting to the board, information disposal standards, and a response program to address incidents of unauthorized access. We will now provide step-by-step instructions for developing your own information security plan.

D. STEP ONE – ASSESSING YOUR RISK

There are essentially four parts to conducting a risk assessment: (1) undertake an information inventory; (2) identify potential internal and external threats; (3) assess the likelihood and potential damage of these threats; and (4) determine if current policies and procedures adequately protect against these threats or if adjustments need to be made.

1. Conduct an Information Inventory

The first step in conducting a risk assessment is to take an information inventory. Each manager should inventory what information his/her area uses, and the way data is obtained, stored, accessed, transmitted, used and disposed of within his or her department, being mindful that there may be multiple ways these are accomplished. For example, in the lending area, customer information is obtained through the application process, and loan applications may be taken through the mail, directly by platform personnel, over the telephone, or through the Internet. Moreover, customer data may be stored, used, accessed, transmitted and disposed of in multiple ways in each unit. The risk assessment should identify each one of these processes in order to accurately portray the risk potential in each department or unit.

Since the various departments or business units within your institution may have different ways of performing these tasks, it would be best if each department or business unit manger conducts the risk assessment for his or her area. However, one individual should be responsible for the process as a whole, be responsible for coordination efforts, and for creating an institution-wide risk assessment.

The following chart will help you conduct the survey and compile the necessary data:

TABLE ONE: CHECKLIST OF ACTIONS IN CONDUCTING INFORMATION INVENTORY

ACTION ITEM	EXAMPLE	FINDINGS
List all of the ways in which your bank or thrift collects personal data.	*Deposit account opening documents, loan applications, trust account files, credit insurance applications, non-deposit investment products.*	
List all the methods in which personal data may be obtained.	*Paper applications, e-mail, web site, telephone calls, U.S. mail, Federal Express.*	
List the methods by which personal data is stored and transmitted.	*Paper files kept in locked filing cabinets, paper files maintained in remote locations, electronic records kept on an off-site computer server, and data is transmitted by e-mail, U.S. mail, inter-office mail and messenger.*	
Identify current controls and limits on access to data.	*Paper files are under lock and key and access controlled by branch manager; the computer system is password protected and only IT manager has access to the passwords. Logs are maintained reflecting access to both paper and electronic files. Internal Audit reviews.*	
For each type of data, determine who needs access as part of their work responsibilities and who, in fact, has access.	*Branch manager has access to all branch files. Loan officer has access to loan applications in his or her portfolio. Data input clerks have access, as do employees at service provider. IT manager has access to all data on computer server. Cleaning crew has access to files kept in desk drawers.*	
List the various ways in which personal information can be accessed.	*Opening file cabinets, accessing computer server.*	
Determine if you obtain customer information through third parties.	*Credit reporting agencies.*	
List the ways data is disposed of.	*Shredding, deleting computer files, municipal trash pick-up, and private trash pick-up*	

2. Identify Reasonably Foreseeable Threats

The next part of your risk assessment is to review your information inventory and evaluate how that information could be compromised through an internal or external threat.

A. Internal Threats

The potential for internal threats is influenced by a financial institution's business practices. For example, the more employees with access to customer data, the greater the internal threat potential. Similarly, multiple data gathering or data storage practices also increase the internal threat potential. Therefore, in review for internal threats, you should:

- Identify the internal staff that have access to personal data identified in the inventory and determine if any of those individuals has access to more data than is necessary. Employees with access to data in transit should also be identified.
- Identify the duplicative or overlapping information gathering and storage systems, and determine if such duplication is necessary.
- Internal threats to data stored or disposed of internally must also be captured in this part of the risk assessment.

B. External Threats

External threats arise from the transmission of data outside of the institution, as well as attempts to penetrate the bank’s security system by outside parties, such as computer hackers. External threats also include damage to data caused by outside forces, such as a fire or flood. Therefore, in review for external threats, you should:

- List the reasons and ways in which personal data is transmitted out of the institution, such as the transmittal of information to loan closing agents, correspondent banks, and securities firms. Identify the ways data is transmitted to other locations within the institution (e-mail, inter-office mail).
- Identify the ways in which the bank’s computer system is connected to the outside, for example, through networks or e-mail.
- Identify the personal data to which third party service providers have access or control.
- Consider the extent to which personal data could be damaged by fire, flood, computer malfunction, or electrical surges or power outages.
- External threats to data stored or disposed of by service providers must also be captured in this part of the risk assessment.

E. ASSESS THE LIKELIHOOD AND POTENTIAL DAMAGE OF IDENTIFIED THREATS.

The last part of your risk assessment is to assess the likelihood of potential damage of identified threats. One method to accomplish this is for each department or business unit manager to score from one to ten the data in his or her department, based on the potential harm or inconvenience that could result if the data was released to an unauthorized party.

TABLE TWO: HYPOTHETICAL RISK ASSESSMENT SCORE

Information	Score
Social security, bank account numbers and passwords	10
Information on current earnings	9
Sources of income, such as alimony payments	8
FICO Score	6
Name and current address	5
Name of current employer	3
Telephone number	2

Based on the total score for each information storage area or system, prioritize the sensitivity of the information stored in that area, and determine the information storage areas and systems that are most sensitive and important to protect.

F. STEP TWO – DETERMINE IF ADJUSTMENTS ARE NEEDED IN CURRENT POLICIES AND PROCEDURES DESIGNED TO PROTECT AGAINST THESE THREATS

Management needs to ensure that controls promote the objectives of the customer information security guidelines. To establish the importance of customer information security, your institution should develop an institution-wide customer information security policy that each business unit will have to follow. In order to comply with the policy, each business unit will have to develop procedures, business practices, and internal controls that address the policy requirements.

The institution's customer information security policy must be approved by the board or a board committee, and should address all of the topics contained in the guidelines.

The following list contains ideas on how some of the guideline topics could be addressed in a policy statement.

- A statement reflecting the institution's desire to safeguard customer information by adhering to regulatory standards.
- Definition of what is considered "customer information."
- Identification of threats to records.
- Limitations on access to customer records.
- Physical security requirements.
- Protection against electronic intrusion. The customer information security policy statement should recognize if and where customer records are vulnerable to electronic intrusion (either through "hacking" or from unauthorized telephone inquiries).
- Frequency of internal and external audit review of customer information security standards.
- Standards that third party servicers will be required to meet. The policy should also discuss the financial capacity of the service providers; the providers' reporting requirements to the institution, and what type of security measures the providers should take to meet regulatory guidelines.
- Disposal procedures and safeguards.
- Employee training.

The policy statement should include a requirement for a periodic review of the customer information security program. Management should be aware of changes made to any part of bank operations that could impact customer information security. As operations change, there should be a process in place to determine if the change impacts customer information security. Common factors that could result in modification include changes in technology, changes in the customer base, new business practices, and new or additional service providers.

Sample Institution-Wide Information Security Policy

It is the policy of Community Bank and Trust to protect the nonpublic personal financial information of all of our customers, and to have a customer information system that includes administrative, technical, and physical safeguards. These safeguards are intended to ensure information security and confidentiality, protect against threats, protect against unauthorized access, and ensure proper disposal of all documents containing non-public consumer information. We consider all consumers who have a continuing relationship with our institution to be our customers.

We will take appropriate steps to comply with regulatory guidelines, and we will by contract require that third parties we employ, who have access to customer information, also comply with these guidelines. We will protect all information that our customers provide in the course of doing business with our bank, except for information that is otherwise publicly available.

To this end:

- The Bank will determine, on an on-going basis, potential threats to the security of our customers' confidential information.
- Access to confidential customer information will be limited to those employees who have a need to access such data in carrying out official responsibilities.
- All employees with access to such data will receive training in information security and the requirements of the Inter-Agency Standards for Safeguarding Customer Information.
- The Bank will house confidential customer data in a manner that provides adequate security, whether the data is in paper form or computer files.
- Internet and other electronic connections to third parties will be protected from intrusion and manipulation using the most appropriate safeguards and systems.
- Before entering into any business arrangements with third party service providers who will have access to customer information, the institution will conduct due diligence to assess the provider's security environment and financial capacity.
- Third party providers will be required to abide by the Inter-Agency Standards.

- Confidential customer information will be properly disposed of as mandated by the Inter-Agency Standards. Information obtained from individuals who do not become institution customers will also be disposed of as mandated by the Inter-Agency Standards.

- Customer information security procedures and controls will be reviewed through an internal audit at least annually, and at least once every two years as part of our external audit. Any defect or deficiency will be promptly remedied.

- The customer information policies and procedures will be reviewed and adjusted in light of any changes in the business practices and activities of this Bank or changes in the security environment, either in the form of newly developed threats or newly enhanced security processes.

G. STEP THREE – DESIGNING SECURITY CONTROLS AND PLANS

Based on the risk assessment and the policy statement, management should develop specific controls and security plans for each business unit impacted by the customer information security guidelines. The guidelines contain a list of specific control techniques that financial institutions must consider and adopt if appropriate. It is a best practice, within the security program documentation, to state the reasons for adopting or rejecting each of these techniques. The FFIEC *Information Security IT Examination Handbook* (December 2002) is also a good source for control procedures and regulatory expectations concerning customer information security.

1. Access Controls

Access controls are designed to limit access to information and provide an audit trail identifying those people who accessed customer information. They are designed to require a person to identify him or herself by using some sort of unique identifier before customer information can be accessed. The types of access controls that the regulators have in mind include:

- Authentication procedures such as passwords, personal identification numbers (PINs), and electronic tokens.[2]
- Firewalls and anti-spyware programs for networked electronic databases.
- Biometric identification systems that, for instance, recognize fingerprints or voice patterns.
- Caller identification telephones.
- Limiting physical access to record storage areas.
- Logs, physical or electronic.

The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. When customer

[2] Electronic tokens are devices designed to assist in the authentication of the user. One example is a device given to the user that generates a new password every 30 seconds. The financial institution's computer system is likewise designed to generate the same password for that customer at the same time that the customer logs on. If the passwords match, the customer would be allowed to access the system. However, a token system cannot be relied on alone, since the token could be lost or stolen.

information is in electronic format, security weaknesses often arise when only a single-factor authentication system is used, for example, when access is permitted when a PIN number is presented and no other requirement is needed. Where risk assessments indicate the use of single-factor authentication is inadequate, (e.g. if money is being moved out of the institution) financial institutions should use layered security, or other controls reasonably calculated to mitigate those risks. Layered security may require the use of a password or other information that person knows with either something the person "has" such as an ATM card, *or* something the person "is" such as a fingerprint, voice pattern, or retinal scan.[3]

Examples Of Access Controls:

Paper files: All files containing nonpublic customer information are to be kept in locked drawers or in a secure filing room. Only authorized personnel will have keys. With respect to the filing room, a log will be maintained of all personnel who enter, and a record made of any files removed and date returned.

Computer: Access to network will be protected by firewall systems supplied by XYZ Corporation. The network will be segregated into security domains, so that access to one domain will not provide access to unauthorized domains. Access will require Password and PIN, and will be limited to the appropriate domain for that user. An electronic log will be maintained of access to files containing confidential customer information. Access to stand alone computers will be controlled through passwords and PINS, and these computers will be protected by firewalls and anti-spyware and anti-viral programs.

E-Mail: Confidential customer information will be provided in E-Mail only to customers who know their password, PIN, and another fact that would be in their exclusive knowledge, such as the amount of their last deposit or balance on their home loan.

Phone: Confidential customer information will be provided over the telephone only to customers who know their password, PIN, and another fact that would be in their exclusive knowledge, such as the amount of their last deposit or balance on their home loan.

[3] The latest information on the need to use a multi-layered approach for sensitive transactions may be found in the FFIEC guidance "Authentication in an Internet Banking Environment (2005).

2. Encryption of electronic customer information

If your institution has a significant amount of customer data in electronic format, the data should be encrypted. Information security experts currently consider 128-bit encryption as appropriate, and institutions should use at least that level of encryption. Smaller institutions frequently do not build their own data systems, so the data service provider should be required to encrypt the information at no less than the 128-bit standard. If the provider cannot guaranty adequate encryption, then a new provider should be found.

3. Dual Control, Separation of Duties, and Background Checks

Dual control and separation of duties are bedrock control concepts that should be applied to customer information security. Customer information should not be under the control of one employee. Optimally, dual control would require more than one employee be present to conduct a task. Separation of duties means that one employee does not have the ability to control multiple steps of a process. In a customer information environment this could mean that employees who enter customer data do not make decisions based on that data, or employees who make changes to customer data should not be responsible for notifying customers that changes have been made. After checking applicable laws, background checks for employees with access to customer information should be considered.

Example of Dual Controls and Separation of Duties for a Community Bank

- Loan officers are required to obtain a key or pass code from the head teller to access secure file room.
- IT personnel may not transmit data to service provider unless compliance officer certifies that the data has been encrypted.
- Customer address changes must be verified by a second employee before the change can be activated.

4. Staff Training

Training is a critical component of your bank's customer information security controls. Management should document the training of staff who have access to confidential customer information, and identify staff who need additional training. Suggested training topics include:

- The details of your institution's written policies and procedures on the disclosure and protection of customer information.
- Common techniques used to breach security, such as pretext calling.
- Identifying sensitive customer information.
- Information disposal procedures.
- Password and log in protocols (electronic and physical).
- Employees must know how and to whom to report suspicious activity.
- Employee responsibilities under the unauthorized access response plan.
- Employees should be trained to implement the institution's written policies and procedures governing the disclosure of customer information, and should be informed not to deviate from them.

Staff who build or maintain computer systems or networks containing customer information require additional training. Management should evaluate the training this staff obtains and ensure that resources allocated toward customer information security training are adequate. Management should ascertain that IT staff have received the latest available training and information regarding information security.

Examples of Acceptable Methods of Training

- Outside seminars.
- Training programs offered at local community colleges.
- "At desk" computer-based training.
- In house seminars with professional trainers or in house experts.

5. Monitoring Systems

Management should be able to answer the question, “How will I know if an unauthorized access has taken place?” Software programs that monitor account activity can be an efficient way of detecting intrusions into networked or electronic customer information databases. These programs look for unusual activity in the database. For example, these programs can cut off access if the wrong PIN number is used more than three times in sequence, put a “hold” on unusual requests, such as withdrawals in excess of pre-determined limits, or transfers of funds to certain high risk countries. If a third party servicer is used to house data electronically, the institution should assure itself that the service provider is conducting this type of control.

Employees should also be trained to identify unusual activity that may signal attempts to gain access to information in ways other than through a computer (e.g. information requests without full identification, frequent telephone requests in a short time) for in person or telephone contacts. “Stand alone” computer databases in PCs must also be monitored.

Table Three: Sample Partial Checklist To Identify Access-Monitoring Controls For The Deposit Area

EMPLOYEE COMPUTER ACCESS	
Must employees enter a password to gain access to customer information contained in the deposit system?	
Are there defined protocols for these passwords (i.e. number of characters, required non-alpha character)? Are passwords reviewed for protocols?	
Are passwords required to be changed periodically? Do passwords become inoperative if not changed or used?	
Are logs maintained capturing all employee access? Are these logs reviewed on a routine basis?	
CUSTOMER TELEPHONE INQUIRY	
Can customer deposit information be given out over the telephone? If so, how must the caller prove his/her identity?	
Is a record of the date of all customer inquiries maintained? If so, can this be viewed while the employee is on the phone with the inquirer (this would aid in identifying suspected pretext calls)?	
If customer PINS are used, are there rules addressing length and character type?	

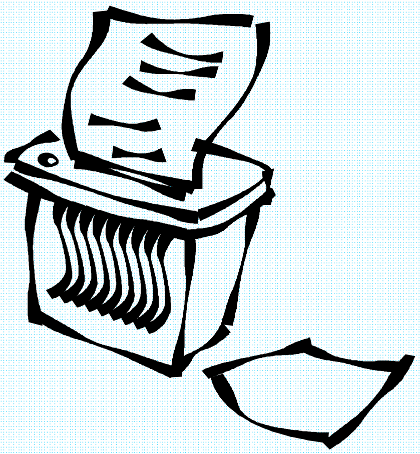
This checklist should be expanded to capture all access points in all areas that hold customer information.

6. Physical and Environmental Hazards

Customer records should be protected against loss due to physical risks (fire, flood) and issues like power failure. The institution's emergency preparedness plans should address customer information concerns. Physical files should be in fireproof files or vaults, and should be watertight. Electronic files should be backed up daily, and power generators should be in place to keep crucial electronic systems functioning.

H. STEP FOUR - DISPOSAL OF CONSUMER INFORMATION

Unlike the standards governing the privacy of nonpublic customer information, the disposal guidelines are applicable to "consumer" information, even if the consumer never became a customer of the bank or thrift institution. In particular, these standards govern any record about an individual, whether in paper, electronic, or other form, that is a consumer report or contains information derived from a consumer report. There is no exception for information that is non-sensitive or otherwise publicly available. However, records that do not identify an individual are not covered. Despite the fact that the guidelines do not cover information that is not derived from a consumer report, it is best practice to use appropriate disposal techniques for all nonpublic consumer information, whether or not required by these standards.



The guidelines require that, as part of an institution's information security program, appropriate measures are taken to dispose of consumer information. The most common way of accomplishing this is through shredding. However, most institutions do not encounter difficulty in shredding the documents they have identified, rather problems arise in *identifying* all of the items that need to be disposed of. It is crucial to identify the areas that have customer information disposal needs. Departmental or business unit management must also identify threats that arise from disposal procedures. For example, the more types of media used to store information, and the more people and places involved in the disposal process, will complicate compliance. Moreover, the type of data that is disposed of is a significant determinant in assessing the likelihood of harm to consumers, furthering the need for the data inventory. The institution's risk assessment should identify the business units that dispose of customer information, and through training, employees should know what records are covered and how they should be disposed of.

Management should be aware of "intermediate" media that contains customer data. For example, a loan applicant may provide information on a paper application that is then entered into an electronic format. Proper disposal techniques must be in place for that intermediate application.

Electronic records pose more difficult problems because even after deletion, residual data is commonly left behind. The institution needs to be aware of this and take additional steps when disposing of sensitive electronic data, such as always retaining the hardware such information was stored in.

Since the regulatory information disposal guidelines apply to all consumer information, management must identify where personal data exists relating to non-customers. This most commonly occurs when a prospective customer either refuses, or does not qualify for, an institution product. Examples include people who do not qualify for loans, or people who turn down loan offers.

I. STEP FIVE – DESIGNING A RESPONSE PLAN FOR SECURITY BREACHES

The guidelines require that institution management develop a response plan when it suspects customer information has been accessed by an unauthorized entity. The person whom the board designated as responsible for the customer information security program should create this plan and be given the authority to designate responsibilities for specific tasks to bank personnel. The response plan should be a written plan. Among the items the response plan should include are:

An evaluation of the extent of the compromise.

- A delineation of responsibility of institution personnel. The plan needs to specify what bank personnel are to do when data is thought to be compromised.
- The response should have procedures to contain the situation. The procedures will depend on the nature of the breach. For example, if data is compromised as a result of unauthorized phone access, the response may be to close the call center until corrective measures are taken. If the data is compromised because of computer "hacking," disconnection from all networks may be appropriate.
- The response plan must include contact information for the appropriate law enforcement agencies, and contact procedures for the primary federal regulator, including completing a Suspicious Activity Report (SAR). As noted above, an institution employee should be responsible for making the appropriate contacts.

- The response plan must also have steps detailing when and how customers will be contacted. If sensitive information (name, address, telephone number in conjunction with social security numbers, drivers' license numbers, credit or debit card numbers, account passwords) is compromised, then customers should be notified. Financial institution management should ensure that notification does not interfere with any law enforcement investigation, so check with law enforcement prior to notifying customers. Management should also be prepared for news media contact. Unauthorized access of customer information, on any significant scale, is a news item, and the institution should be prepared to communicate with the media to contain reputation risk.

J. STEP SIX – OVERSEEING A SERVICE PROVIDER

Smaller institutions are increasingly relying on third party service providers to manage and store data. The interagency customer information security guidelines require that each contract between a financial institution and service providers with access to customer information contain the following:

- Language that requires the service provider take appropriate measures to protect the data from unauthorized access.
- A requirement that the service provider have a response plan in the event information is accessed by an unauthorized party.
- A clause that requires the service provider to properly dispose of customer information.

Essentially, by contract, the service providers must agree to follow the regulatory standards, and the institution has to assure that the service providers keep to the agreement.

When entering into a contract with a service provider who has access to the customer data, the following specific contractual factors should be included:

- The contract contains adequate and measurable customer information security standards (for example requiring 128-bit encryption, the use of "XYZ" firewall etc.).
- The rights and responsibilities of both parties are sufficiently detailed.

- Notification about subcontracting arrangements.
- Contract clauses addressing significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, continuity of service, etc.
- The type of reports and the frequency of submission that the provider must send the institution.
- A requirement that the provider implement appropriate measures to meet regulatory customer information security standards.

Legal counsel should review the contract with the service provider, and any issues raised during this review should be satisfactorily resolved.

The financial institution must conduct adequate due diligence before contracting with a service provider. Due diligence standards addressing a service provider's financial and operational capacity are addressed in other supervisory issuances. The customer information security guidelines require that due diligence be expanded to address a service provider's security procedures. Due diligence requirements encompass all material aspects of the customer information security guidelines, specifically addressing the following:

- Reputation (e.g., reference checks)
- Controls.
- Key personnel.
- Disaster recovery plans and tests.
- The use of subcontractors.

The financial institution should develop monitoring procedures to verify that all service providers are safeguarding the institution's customer information. The institution should receive and review relevant information from service providers. The contract should include the requirement that the financial institution receive relevant information. Such information includes the following:

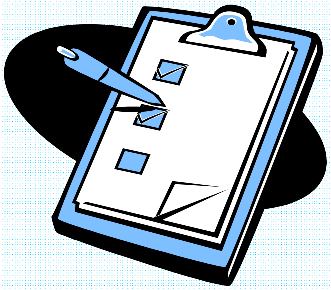
- Operating procedures.
- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports.

- Corrective measures for audit or regulatory report findings.
- Information security practices, standards and procedures.
- Financial information necessary to assess capacity and viability.
- What personnel at the provider will conduct these tasks, and their qualifications for performing them.

Your periodic monitoring of the service provider should be conducted in a timely manner. Information should be analyzed soon after it is received. The timing of the review should reflect changes in the risk due to altered circumstances at the service provider, including financial and control changes. Your review should address the provider's conformance with the customer information security requirements in the contract. You should be aware of any subcontracting arrangements (the contract should require notification) and take appropriate steps to monitor the subcontractors.

Steps in Monitoring Service Providers

- Monitoring of service provider will be conducted on a quarterly basis.
- The service provider will be asked to confirm that it is complying with all required security requirements.
- The service provider will list any new or different sub-contracting arrangements.
- The service provider will report on any updates or changes in security procedures or devices.
- The service provider will report any adverse events, security breach attempts, and actual breach events.
- The provider will certify that all appropriate employees are up to date on training, and that security checks have been completed on any new employees.



The following checklist will also be helpful in monitoring third party providers:

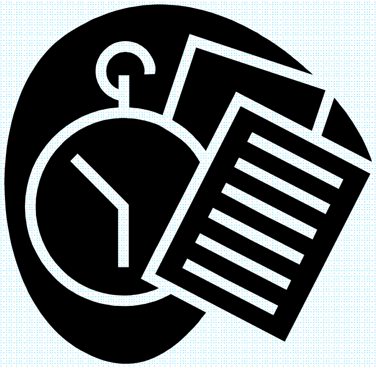
Table Four: Third Party Servicer Oversight Checklist

TOPIC	REFERENCE DOCUMENT	REVIEWED BY
Servicer's unauthorized access response plan		
Servicer's customer information disposal procedures		
Servicer's financial statements		
Contractual clause includes measurable customer information security standards		
Permissible subcontractor activities and notification requirements		
Financial and other reporting requirements		
Ownership of customer data contract clause		
Reference check on servicer		
Servicer's firewall		
Servicer's encryption standard		
Servicer's disaster recovery plan		
Key personnel at servicer and responsibilities		
Acknowledgment by servicer to adhere to regulatory standards		
Notification of financial institution by the servicer that an unauthorized access has occurred		
Attorney review of contract		

K. STEP SEVEN – TESTING

As part of the risk assessment, the scope, frequency, and sequence of security control testing should be established. The guidelines require that customer information controls be reviewed in a coordinated fashion and address all the issues in the guidance. So while control steps may be taken in conjunction with another activity, the results of the controls and testing need to be specifically incorporated into the customer information security review.

Control testing must be conducted by a party independent from the area being tested, and must not have been involved in the creation of the customer information control system.



Examples of Control Tests

- Unscheduled mock pretext telephone calls.
- “Ethical hacking” tests.
- Review of reports addressing expired passwords.
- Review of activity in customer databases.
- Review of customer information file access logs.
- Internal and external audit reports.

CONCLUSION

Information security is a critical component of every financial institution's compliance responsibilities. This is often viewed as a complex and challenging requirement. However, if you follow the guidance in this document, you should be able to develop the appropriate policies and procedures that to comply with regulatory requirements and protect the information your customers have entrusted to your organization. It is important to remember that this is a fast changing area, and new technical and regulatory developments are frequent. You should be alert to changes in regulatory requirements that may be mandated by the Congress or the agencies, as well as to new techniques to breach security protections and the latest techniques to defend against such breaches.